
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

-v-

Mag. No. 09-3103

BRUCE RAISLEY

I, Susan Secco, being duly sworn, state the following is true and correct to the best of my knowledge and belief. From in or about July 2007 to in or about March 2008, in Hudson County, in the District of New Jersey and elsewhere, defendant BRUCE RAISLEY did:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.



Susan Secco, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
June 29, 2009, in Essex County, New Jersey

HONORABLE PATTY SHWARTZ
UNITED STATES MAGISTRATE JUDGE


Signature of Judicial Officer

ATTACHMENT A

Between in or about July 2007 and in or about March 2008, in the District of New Jersey and elsewhere, defendant

BRUCE RAISLEY

knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, that is, one which was used in interstate commerce and communication, and by such conduct caused loss to one or more persons during a 1-year period aggregating at least \$5,000 in value.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and 1030(c)(4)(B)(i).

ATTACHMENT B

I, Susan Secco, a Special Agent of the Federal Bureau of Investigation, have knowledge of the following facts based upon my investigation and discussions with witnesses and other law enforcement agents. Since this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a complaint and arrest warrant, I have not included each and every fact known by the government concerning this investigation. Statements attributed to individuals are provided in substance and in part.

BACKGROUND

1. Definitions:

a. Bot: A bot is an automated computer program that repeatedly performs a specific function. Bot programs can perform useful tasks, such as regularly updating weather and traffic conditions on local news websites or scanning the Internet to update comparison shopping websites. They can also perform destructive tasks such as scanning the Internet for unsecured computers for the purpose of identifying and sometimes installing computer viruses or other destructive programs. These compromised or “zombie” computers can then be used to repeatedly attack a domain or IP address on behalf of the bot originator or “bot herder.”

b. Botnet: A collection of bots is a “robot network” or *botnet*. A *botnet* is typically remotely controlled by the bot herder using a “command and control” server. A command and control server is an Internet-connected computer to which the bot herder issues instructions, which in turn sends those instructions to the bots controlled by the bot herder. A botnet is generally comprised of thousands, sometimes hundreds of thousands, of computers.

c. Distributed Denial of Service (DDOS) Attack: A DDOS attack involves the use of a large network of computers, commonly a botnet, to simultaneously flood a victim website with either repeated requests for information or “junk” data, either one of which could flood the site with too much information and effectively cripple it. The perpetrators of DDOS attacks gain control of large numbers of computers to use in this type of attack, commonly by assembling a botnet. Once the botnet is in place, when used for a DDOS attack, the botnet awaits orders from the command and control server. To receive these orders, a botnet often checks back with the command and control servers or uses preexisting commands to act.

2. At various times relevant to this Complaint:

a. Defendant Bruce Raisley resided in Searcy, Arkansas and subsequently moved to Monaca, Pennsylvania.

b. The Rick A. Ross Institute of New Jersey (the “Rick Ross Institute”)

maintained a website, www.rickross.com, entitled the “Rick Ross Institute Internet Archive for the Study of Destructive Cults, Controversial Groups and Movements.” The Rick Ross Institute was based in Hudson County, New Jersey.

c. Perverted Justice was a Portland, Oregon based organization operated by X.E., which sought to identify and expose pedophiles and sexual predators targeting minors. Perverted Justice members were civilian volunteers who assumed online identities as minors, and, after engaging in sexually explicit online conversations with other individuals whom they believed to be adults, attempted to fully identify those individuals. Perverted Justice then posted the individuals’ information and explicit online conversations on their website. Because of its operations, Perverted Justice attracted detractors who claimed that it was a vigilante operation. In or about 2004, defendant Raisley was a volunteer with Perverted Justice.

d. Corrupted Justice was an organization whose stated purpose was to educate the public by providing details and information regarding the actions of various purported cyber-vigilante groups in operation on the Internet, including Perverted Justice. In or about 2006, defendant Raisley was a volunteer member of Corrupted Justice after he ceased being a volunteer at Perverted Justice.

DEFENDANT RAISLEY AND PERVERTED JUSTICE

3. In or about September 2006, Radar Magazine published an article by John Cook entitled “*Strange Bedfellows*.” In or about July 2007, Rolling Stone published an article entitled, “*To Catch a Predator: The New American Witch Hunt for Dangerous Pedophiles*” (the “*New American Witch Hunt*”). The *New American Witch Hunt* was featured in an August 2007 edition of the Rolling Stone magazine. Both *Strange Bedfellows* and *New American Witch Hunt* presented positive and negative views of the activities conducted by Perverted Justice and its volunteers, and described what was termed as “questionable tactics” by Perverted Justice to silence critics. One of the “questionable tactics” in the articles was an episode between X.E. and defendant Raisley.

4. In or about 2007, *Strange Bedfellows* was reprinted on numerous websites, including Corrupted-Justice’s website, www.corrupted-justice.com; Radar Magazine’s website, www.radaronline.com; and the Rick Ross Institute’s website, www.rickross.com. The *New American Witch Hunt* was likewise reprinted on numerous websites and remained on the Rolling Stone’s website, www.rollingstone.com (the websites reprinting the articles, collectively, the “Reprinting Websites”).

THE RICK ROSS INSTITUTE DDOS ATTACK

5. On or about September 25, 2007, the Rick Ross Institute’s website experienced a DDOS attack. During the DDOS attack, the URL hosting *Strange Bedfellows*,

http://rickross.com/reference/perverted_justice26.html, experienced repeated hits from thousands of IP addresses.

6. One of the bots unwittingly conducting the attack against the Rick Ross Institute's website was assigned IP address 153.5.60.232. That IP address is registered to Academic and Research Network of Slovenia (ARNES) in Ljubljana, Slovenia. One of the services offered by ARNES is the Slovenian Computer Emergency Response Team (SI-CERT). SI-CERT provides computer security services to its members, which include "coordination of security incidents involving networks or systems in Slovenia, distribution of security-related information to the constituency, and providing technical expertise on network security related issues."

7. After being notified of the possible compromise of the computer assigned IP address 153.5.60.232, SI-CERT officials examined the computer and located on it a malicious program detected by virus and malware detection programs as one capable of being part of a botnet (the "Bot Malware.")

8. On or about November 20, 2007, technical personnel at SI-CERT analyzed the Bot Malware and determined that it was designed to access the internet and download instructions as to its function. In particular, SI-CERT determined that the program downloaded its instructions from two locations, www.dosdragon.com, which was hosted on a computer server assigned IP address 68.178.232.100, and www.n9zle.com, which was hosted on a computer server assigned IP address 208.109.162.16 (the "Command and Control Systems"). SI-CERT further determined that if the Bot Malware was unable to receive instructions from the Command and Control Systems, it was instructed to repeatedly target certain websites. Among the websites targeted by the Bot Malware, all of which carried either *Strange Bedfellows* and *New American Witch Hunt*, were:

- a. www.radaronline.com/features/2006/09/strange_bedfellows;
- b. wyldemusick.livejournal.com;
- c. www.corrupted-justice.net;
- d. www.superpatriot.net;
- e. www.perverted-justice.com;
- f. www.rickross.com/reference/perverted_justice26b.html;
- g. www.cleolinda.livejournal.com/451308.html;
- h. www.rollingstone.com/news/story/15723886/to_catch_a_predator_is_nbc_primetime_dragnet_the_new; and
- i. www.kardasz.org/cybervigilantes2.html.

9. Rolling Stone's website was the subject of multiple DDOS attacks directed specifically at the webpage hosting *New American Witch Hunt* from in or about July 2007 and continuing through in or about March 2008. During the height of the DDOS attacks, the page requests for the article escalated from a few page requests per day to millions of page requests per day, causing the website to experience significant slowdown.

10. On or about March 7, 2008, the United States Computer Emergency Response Team (US-CERT) confirmed through their reverse engineering of the Bot Malware that it was downloading attack instructions and target lists from the domains n9zle.com and dosdragon.com. The Bot Malware was distributed using the file "vdriver.exe."

11. On or about January 16, 2008 and February 8, 2008, the FBI received records from internet service providers which revealed that defendant Raisley controlled both Command and Control Systems.

CORRUPTED-JUSTICE DDOS ATTACKS

12. On or about July 5, 2007, Corrupted Justice's website, www.corrupted-justice.com, was the victim of a DDOS attack which shut down the website for four days. At that time, the website contained a copy of both *Strange Bedfellows* and *New American Witch Hunt*.

13. On or about November 2, 2007, Corrupted Justice's website was subjected to a second DDOS attack that lasted approximately three days. S.M., an administrator of the Corrupted Justice website, informed the FBI that defendant Raisley contacted him over the Internet to "gloat that he had again taken down [Corrupted Justice's] servers."

14. On or about March 10, 2008, Corrupted Justice's website was subjected to a third DDOS attack that lasted approximately four days. During the March 2008 attack, Corrupted Justice's website was taken offline, as were other commercial and business websites hosted on the same server.

15. On or about the date of the March 2008 attack, S.M. contacted defendant Raisley by telephone. According to S.M., Raisley stated that he "unleashed a virus that could never be stopped," that S.M. could "kiss [his] website goodbye because nothing could protect [his] servers against this attack," and that S.M.'s "website is finished forever."

DEFENDANT RAISLEY'S HOUSE IS SEARCHED

16. On or about March 27, 2008, the FBI executed a search at defendant Raisley's residence in Monaca, Pennsylvania (the "March 27, 2008 Search"). The FBI recovered computers and electronic media during the search, including a 2 gigabyte memory stick (the "Memory Stick") and a 40 gigabyte external hard drive.

17. During the course of the March 27, 2008 Search, defendant Raisley spoke with the FBI agents and claimed that he had been harassed for years by Perverted Justice. He then directed the FBI agents to a copy of an August 2007 Rolling Stone magazine in his bedroom which included a flagged copy of the *New American Witch Hunt*. Defendant Raisley then stated

that he had indeed spoken with representatives at the Rick Ross Institute and Corrupted Justice and asked that copies of the articles be taken down from their websites. When asked if he had been responsible for launching DDOS attacks on the websites, Raisley stated that he was “not controlling bots from [his residence], period.”

18. As the FBI concluded the March 27, 2008 Search, Raisley was asked again if there was anything further he wanted to state. Raisley replied: “The memory stick you took has on it everything you need.” He further stated that he wrote the programs on the Memory Stick. Finally, defendant Raisley stated that he used the programs on the Memory Stick to attack the websites of Perverted Justice, Corrupted Justice and the Rick Ross Institute.

19. The FBI conducted a forensic review of the seized electronic media, including the Memory Stick and confirmed that it contained copies of programs used in conjunction with the DDOS attack described above.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

-v-


BRUCE RAISLEY

:
:
: **SEALING ORDER**
:
: Mag. No. 09-3103
:
:
:

An application having been made by Ralph J. Marra, Jr., United States Attorney (Erez Liebermann, Assistant U.S. Attorney, appearing), for an Order sealing the complaint, arrest warrant and accompanying papers until the arrest of the named defendant, and good cause having been shown,

IT IS on this 29th day of June 2009,

ORDERED, that the complaint, arrest warrant and accompanying papers are sealed until the arrest of the defendant or until further order of this Court.


HONORABLE PATTY SHWARTZ
United States Magistrate Judge